



(12)

# EUROPEAN PATENT APPLICATION

(43) Date of publication:  
01.07.1998 Bulletin 1998/27

(51) Int. Cl.<sup>6</sup>: H04L 9/08, H04Q 7/32

(21) Application number: 96309444.6

(22) Date of filing: 23.12.1996

(84) Designated Contracting States:  
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC  
NL PT SE  
Designated Extension States:  
AL LT LV

(72) Inventor:  
Johnston, Thomas Francis  
London, W2 6DG (GB)

(74) Representative:  
Read, Matthew Charles et al  
Venner Shipley & Co.  
20 Little Britain  
London EC1A 7DH (GB)

(71) Applicant: ICO Services Ltd.  
London W6 9BN (GB)

## (54) Key distribution for mobile network

(57) A satellite mobile telecommunications system includes mobile terminals 2a, 2b which can communicate with one another using end-to-end encryption and decryption techniques. When secure end-to-end communication is required, each terminal uses a common encryption code (RAND) to encode data and decode data transmitted between the terminals. The encryption code is transmitted in a secure manner from a remote database station (15) to the terminals. Each terminal stores a terminal key ( $K_a$ ,  $K_b$ ) on its SIM card and the keys are also held in the remote station (15). Partial keys ( $K_{pa}$ ,  $K_{pb}$ ) comprising the pseudo random number (RAND) and the keys  $K_a$ ,  $K_b$  stored at the station (15)

are produced at the station (15) by an exclusive OR process in order to mask the keys and the random number. The partial key  $K_{pa} = K_a + (RAND)$  is sent to terminal 2a. At the terminal 2a, the partial key  $K_{pa}$  is exclusive OR-ed with the locally stored terminal key  $K_a$  on the SIM card, so as to recover (RAND). The common code (RAND) is determined by the same process at terminal 2b, from  $K_{pb} = K_b + (RAND)$  and the locally stored key  $K_b$ . The terminals then both run a GSM encryption algorithm (A5) to encrypt and decrypt transmitted data, on the basis of the common code (RAND).

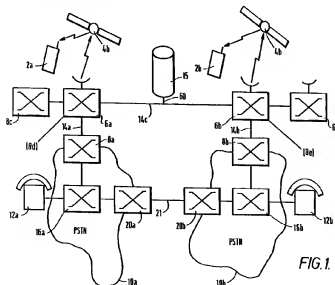


FIG. 1





























































